Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] What is claimed is:

1. A multilevel custom secured computer system comprising:

A custom-built computer case with lockable front and back covers using high-level security key/locks, and fourteen (14) hardware slots within the case, two separate motherboards with their own independent central processor units (CPU), random access memory (RAM), video card, network interface card (NIC) within each domain, two separate hard drives (one within a removable hard drive case), two separate floppy disk(s) and CD-ROM(s) drive(s), and a keyboard, video, mouse, (KVM) switch for switching keyboard, video and mouse functions between the two separate domains;

The first computer domain within this custom-built case is identified as the UNSECURED DOMAIN, having an optional fax/modem which allows data communications via the Internet, and the ability to operate independently with its own central processing unit (CPU), network interface card (NIC) for connecting to an unsecured network, video card, hard drive, floppy/CD-ROM drive(s) labeled with a green mark for easy identification, operat-

ing system (OS), and random access memory (RAM);
The second computer domain within this custom-built case is identified as the SECURED DOMAIN, having a Smart Card® reader/writer that reads and process access requests and provides identification and authentication for authorized users having a Smart Card® reader/writer token, and the ability to operate independently with its own central processing unit (CPU), network interface card (NIC) for connecting to a secured network, video card, removable hard drive with a lock/key, (for storing secured data and is removable to be stored in a safe after each use) floppy/CD-ROM drive(s) labeled with a red mark for easy identification, operating system (OS), and random access memory (RAM);
An electro-mechanical lock/key on the front of the case for powering-on both computer domains and cannot be removed unless the system is powered off;
A green reset button in the front of the computer case which provides the reset function for the unsecured domain;
A red reset button in the front of the computer case which provides the reset function for the secured domain;
2. The multileveled custom secured computer system as set forth in claim 1, with said first computer domain including a central processing unit (CPU), random access

memory (RAM), hard disk drive, floppy/CD-ROM drives, network interface card, random access memory, video card, sound card and optional modem.

[c2] 3. The multileveled custom secured computer system as set forth in claim 1, with the second computer domain including a central processing unit (CPU), random access memory (RAM), removable hard disk drive, floppy/ CD-ROM drives, network interface card, random access memory, video card, optional sound card, Smart Card® reader/writer for user access control and identification and authentication.

[c3] 4. A lockable front cover as set forth in claim 1 provides a hardware-based access control to the multileveled custom secured computer case using a high-level security lock/key.

5. A lockable back cover as set forth in claim 1, with two separate cable outputs which allows color-coded network cables to remain separate and identified, a high-level mechanical lock/key for preventing cable interchange or removal.

6. An electro-mechanical high-level security lock/key which is connected to the ON/OFF function of the main computer case power supply will activate and power-on both computer domains when the authorized user inserts the high-level security key. The key of said electro-

mechanical high-level security lock must be inserted and turn clockwise to the ON position by the authorized user first. The unsecured domain will be accessible first by default without any other access control requirement. It is impossible to turn-on the multileveled custom secured computer without the key. The key cannot be removed in the ON position. It can only be removed in the OFF position, when both, the secured and unsecured domains are no longer in use and the user has shut down their respective operating systems (OS).

7. A custom-built Y power cable from the computer case power supply provides power to both domains or central processing units or motherboards, the unsecured domain and the secured domain.

8. An aluminum-based electromagnetic field (EMF) shield is placed between the two central processing units (CPU) or motherboards within the case, to prevent data-bleed over between the two domains and networks.

9. The Smart Card® reader/writer as set forth in claim 1 is interfaced and connected only with the secured domain's central processing unit (CPU) or motherboard and provides access control and user authentication and identification ensuring data integrity for the classified data on the removable hard disk drive and network for the secured domain.

10. An external digital electronic switch otherwise de-

scribed as keyboard, video, mouse or (KVM), which is connected directly to both domains, the unsecured and secured, provides instant switching between the two domains without having to shut down the operating systems or loose data on either domain. Two light emitting diodes (LED) on the keyboard, video, mouse, (KVM) switch, one green and the other red, indicate which domain the authorized computer user is operating.

11. The unsecured domain is ON by default upon powering up the multilevel custom secured computer system when the authorized user inserts his high-level security key into the electro-mechanical lock of the front panel of the computer case. On this mode access to the secured domain is not possible.

12. The secured domain can be selected by pressing the red button on the (KVM) switch and access will be allowed only through the use of the Smart Card® reader/writer that will require the authorized user to insert his Smart Card® and subsequently his personal identification number (PIN). Without the use of the authorized user's Smart Card®, it is impossible to access the secured domain removable hard disk drive and secured network.

13. The multi-level custom secured computer system as set forth in claim 6 is mechanically activated with the use of the high-level security key which interfaces with the computer case power supply by sending an activation

signal to power-on both domains concurrently. However, only one domain is operational and accessible at a time.

14. The multi-level custom secured computer system provides high assurance data access control and secured data processing, data storage, and data communications for data at the unsecured domain and data at the secured domain, all within a custom-built high-security computer case. Both, the unsecured domain and the secured domains having their own totally independent (CPU), data storage devices such as hard disk drives, floppy/CD-ROM drives, memory, video, network interface cards, operating systems (OS), are totally isolated and independent and operate simultaneously without allowing data to inadvertently cross over between domains.

15. The secured domain's removable hard drive as set forth in claim 12 incorporates its own hardware-based locking mechanism with a key for removal and storage after each use. The key cannot be removed while the secured domain and hard drive is operational. It can only be removed when the system is powered off on both domains.

16. The two separate domains as set forth in claim 1 require sufficient cooling due the extra internal components that produce heat. A second cooling fan was installed in the front of the multi-level custom secured

computer system which includes a reusable air filter in order to have adequate air circulation within the system.

17. The two separate domains as set forth in claim 1 incorporate two floppy/CD-ROM combo drives each, which are installed into two separate 5 ¼"drive bays. One floppy/CD-ROM combo which is installed into one 5 ¼" drive bay is connected directly to the unsecured motherboard/CPU and can only process data and information for the unsecured domain. A green indicator identifies this floppy/CD-ROM drive for the unsecured domain.

18. The secured domain's floppy/CD-ROM combo as set forth in claim 17 is installed into a separate 5 ¼" drive bay and is connected directly to the secured motherboard/CPU and can only process data and information for the secured domain. A red indicator identifies this floppy/CD-ROM drive for the secured domain.

19. The unsecured domain's floppy/CD-ROM combo as set forth in claim 17 is installed into a separate 5 ¼" drive bay and is connected directly to the unsecured motherboard/CPU and can only process data and information for the unsecured domain. A green indicator identifies this floppy/CD-ROM drive for the unsecured domain.